

### REMARKS

The above amendments and following remarks are submitted in response to the official action of the Examiner mailed March 25, 2004. Having addressed all objections and grounds of rejection claims 1-20, being all the pending claims, are now deemed in condition for allowance. Entry of these amendment and reconsideration to that end is respectfully requested.

The Examiner has objected to the specification in view of a small typographical error. This error has been corrected by the amendment presented above. Applicants wish to apologize for any confusion this error has caused. It is understood that the remaining issues with regard to the specification have been adequately addressed.

The Examiner has rejected claims 1-20, being all pending claims, under 35 U.S.C. 112, first paragraph. In support of his position, the Examiner states:

However, the details of the use of the site specific security profile is not disclosed in the Detailed Description of the Preferred Embodiments, and in fact the section of the Detailed Description concerning the operation of security profiles discloses a mechanism whereby a user submits a service request which results in the execution of a command language script with associated security profile which requires the user to submit a UserID over the World Wide Web in order for the execution of the script to proceed. (Emphasis provided)

The portion of this statement emphasized by the Examiner is not found within Applicants' disclosure.

However, to resolve any possible misunderstanding, Applicants have herewith amended all pending claims to indicate that the "user identifier" and "terminal identifier" have equivalent formats. Furthermore, transfer of the terminal identifier is required, even though the transfer of the user identifier is not. Comparison between the terminal identifier and security profile results in honoring or denial of the requested service. Again, Applicants apologize for any confusion the previous claim language has prompted. The detailed description of the creation and honoring of the "terminal identifier" is found within Figs. 14-15 of the disclosure.

The Examiner has also rejected claims 1-20 under 35 U.S.C. 112, second paragraph, as being indefinite. Specifically, the Examiner suggests that the claims are inconsistent with pages 33-34 of the specification. Clearly, the specification states at page 7, lines 11-13:

This invention will provide a new SignOn capability which allows for site-specific data to be used to identify a user. The site-specific data is converted to a valid UserID/Password by a User Validation service implemented by a site.

Again, from the point of view of the terminal, as discussed at page 7, a distinction is made between a "user identifier" and a "terminal identifier". However, from the point of view of the

data base management system, discussed at pages 33-34, no distinction is or can be made. However, in an attempt to remove any misunderstanding, claims 1-20 have been amended as described above.

Claims 1-4, 6-8, 11-14, and 16-18 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison") in view of U.S. Patent No. 6,237,023, issued to Yashimoto (hereinafter referred to as "Yashimoto") further in view of "Access Control in Federated Systems" by Sabrina De Capitani di Vimercati, et al (hereinafter referred to as "De Capitani di Vimercati"). This ground of rejection is respectfully traversed as to the amended claims.

In alleging the combination, the Examiner states:

De Capitani di Vimercati et al, however, teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

Table 1 is captioned "Security problems and possible solutions". It should be noted that it does not purport to list practical or recommended solutions.

Furthermore, the text specifically indicates that the reader should not implement the solution alleged by the Examiner (i.e., non-identification of the user). The cited text states in part:

However, this approach would require access authorizations to be specified only with respect to remote identities. The approach of always requiring explicit connection to the federation is preferable, in general, since (sic) it allows authorizations on federated data to be specified against identifiers established and managed by the federation administrator.

Thus, De Capitani di Vimercati, clearly teaches one not to implement the key features of Applicants' claimed invention. It continues in the same paragraph:

However, this approach has the drawback of always allowing access to the system and its schema (although, notice not to the information stored in the objects). Moreover, it may result in unnecessary (sic) sending requests to the local systems, which can instead be avoided by access control at the federation level.

Having provided the reasons not to utilize this theoretical approach, the text continues in the very next sentence describes that the disclosure of the paper assumes that the user identifier will always be provided stating:

Let us therefore assume that each user needs to identify himself to the federation.

Therefore, De Capitani di Vimercati actually teaches away from Applicants' invention as disclosed and claimed.

As if to further confuse the issue, the Examiner cites De Capitani di Vimercati, page 93, column 2, second to last paragraph, which adds nothing to the argument. It states:

Network security. Users, through the federation access data distributed at the component database systems via some type of network. It is necessary protect (sic) to all information transferred over the global communication network and standardize the communication methods.

The alleged combination simply does not meet the claimed invention, and instead teaches away from it.

Claims 5, 9-10, 15, and 19-20 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Garrison, in view of Yashimoto, in view of De Capitani di Vimercati, and further in view of "Unisys CSG MarkePlace - The Mapper System" (hereinafter referred to as "Unisys"). This ground of rejection as to the amended claims is respectfully traversed.

In addition to the reasons given above, the Examiner does not meet his burden of proof under MPEP 2143 to provide "motivation" and "reasonable likelihood of success" of the alleged combination. Specifically, there is no showing that such a combination is at all feasible. In fact, the references actually teach away from the alleged combination.

Having thus responded to each objection and ground of rejection, Applicants respectfully request entry of this amendment and allowance of claims 1-20, being the only pending claims.

Please charge any deficiencies or credit any overpayment to

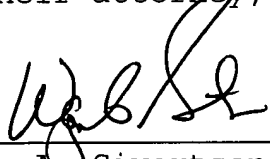
Deposit Account No. 14-0620.

Respectfully submitted,

Paul S. Germscheid, et al

By their attorney,

Date June 24, 2004

  
\_\_\_\_\_  
Wayne A. Sivertson

Reg. No. 25,645

Suite 401

Broadway Place East

3433 Broadway Street N.E.

Minneapolis, Minnesota

55413

(612) 331-1464